



Thomas, NM., Bull, DR., & Redmill, DW. (2009). A novel H.264 SVC encryption scheme for secure bit-rate transcoding. In *Picture Coding Symposium, 2009 (PCS 2009), Chicago, USA* (pp. 1 - 4). Institute of Electrical and Electronics Engineers (IEEE).
<https://doi.org/10.1109/PCS.2009.5167429>

Peer reviewed version

Link to published version (if available):
[10.1109/PCS.2009.5167429](https://doi.org/10.1109/PCS.2009.5167429)

[Link to publication record in Explore Bristol Research](#)
PDF-document

University of Bristol - Explore Bristol Research

General rights

This document is made available in accordance with publisher policies. Please cite only the published version using the reference above. Full terms of use are available:
<http://www.bristol.ac.uk/red/research-policy/pure/user-guides/ebr-terms/>

A NOVEL H.264 SVC ENCRYPTION SCHEME FOR SECURE BIT-RATE TRANSCODING

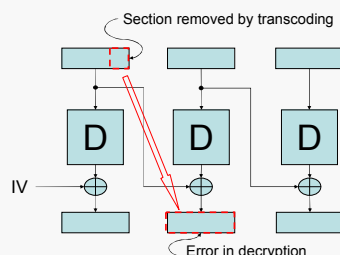
Nithin Thomas, David Bull, David Redmill
University of Bristol, UK

1

ABSTRACT

Motivation:

- Traditional encryption causes **errors** if **transcoding** is carried out
- **ECB** mode encryption not secure
- Adding additional data to preserve synchronization increases **bitrate**



Features:

- **No Decryption** required prior to scaling
- Any **standard cipher** can be used
- Supports all types of **scalability**

Benefits:

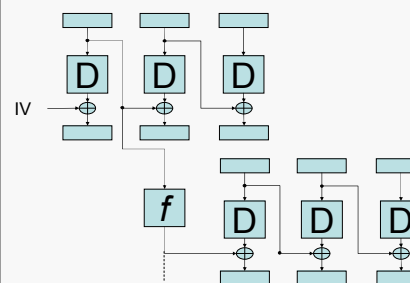
- **End to end** security preserved
- Highest level of **security** using well studied ciphers
- **No bitrate overhead**
- **Compatible** with standard scaling transcoders

2

SVE ARCHITECTURE

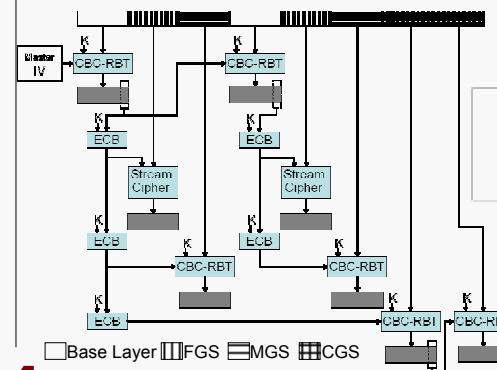
Cipher Block Tree (CBT):

- Novel **mode of operation**
- Allows several **CBC** chains to be connected in a **tree structure**
- Only one **key** and **IV** required to support a tree
- **IV** for a chain created using a function, **f**, on output of block from parent chain



SVE:

- Derived from **CBT** for use with **SVC**
- Support for potential future support of **FGS**
- Uses **Residual Block Termination (RBT)** to avoid bitrate expansion due to **padding**



3

RESULTS

Security:

- **High** level of security
- No weaknesses from **IV reuse**
- No weaknesses from use of **ECB**
- **NAL headers** unencrypted so some information leaked

Transcoder Latency:

- **No latency** added by encryption
- Packets can be **transcoded** **independently** despite encryption

Transcoding Flexibility:

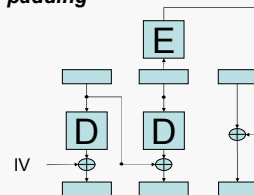
- All forms of **bitrate scaling** supported
- Bit level transcoding using **FGS** is possible
- No effect on the **quality** of output due to encryption

Bitrate Overhead:

- Does not add any significant **overhead**
- Only one **key** and **IV** need to be transmitted
- **Padding** avoided by use of RBT

Residual Block Termination (RBT):

- Standard technique used in **block ciphers**
- Used to encrypt **last block** if size of plaintext is not multiple of block size
- Avoids **bitrate expansion** caused by padding



4

CONCLUSIONS

- An encryption scheme **optimised** for use with **SVC**
- Can be modified for use with other **scalable media**
- Can support **FGS scalability**
- Encryption **transparent** to transcoder
- High levels of **security** possible
- Benefits of **scalable** coding preserved
- No compromise on **codec performance**